Christopher J. Schatz, OSB No. 915097
Assistant Federal Public Defender
101 SW Main Street, Suite 1700
Portland, OR 97204
Tel: (503) 326-2123
Fax: (503) 326-5524
Email: chris_schatz@fd.org

Ruben L. Iñiguez
Assistant Federal Public Defender
101 SW Main Street, Suite 1700
Portland, OR 97204
Tel: (503) 326-2123
Fax: (503) 326-5524
Email: ruben_iniguez@fd.org

Attorneys for Hock Chee Khoo

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA, **Plaintiff,** **vs.** **HOCK CHEE KHOO, et al.,** **Defendants.**	**CR 09-321-KI** **REPLY TO GOVERNMENT'S BRIEF RE MOTION TO EXCLUDE IMAGES OF THE WU LAPTOP AND EXTERNAL HARD DRIVE.**

Defendant Hook Chee Khoo, by and through his attorneys of record, Christopher J. Schatz and Ruben Iñiguez, hereby replies to the Government's Brief Regarding Defendants' Motion To Exclude Images Of The Wu Laptop And External Hard Drive [Docket No. 105]. Insofar as the Court directed that simultaneous filing of the parties' briefs occur [Docket No. 84], the instant Reply is limited to correction of a single, albeit thrice-repeated, misstatement of fact found in the Government's Brief at pp. 4, 9 and 10, and which the government advances as a material component of its claim to have established a *prima facie* case for authentication of the FTK EnCase images of the Wu laptop and the USB device containing the Acronis backup copy. The misstatements of fact set forth in the Government's Brief are as follows:

> Administrative review of the forensic examination also revealed that hash values for both images matched hash values for the original values made of the Wu Laptop and the Acronis copy, indicating that the forensic process resulted in an exact copy of the original.

Government's Brief at p. 4.

> [T]here is no dispute that the forensic images created by the FBI had the same hash values as their original sources, indicating exact copies.

Government's Brief at p. 9.[1]

> In spite of defendants' arguments to the contrary, an administrative review of the forensic process showed that the images were acquired under conditions that were forensically sound, with equipment that was properly calibrated by qualified personnel, **and, finally, that the hash values matched**. Under these circumstances, the government has clearly established a prima facie showing . . ..

Government's Brief at p. 10 (emphasis added).

[1] Of course there is a dispute. It is Mr. Khoo's contention, reiterated again and again in his pleadings and through the un-refuted testimony of Computer Forensics Expert Michael Bean that, as a consequence of Hoffman's spoliation (which the FBI could have prevented), the FTK EnCase images do not constitute duplicate originals of the Wu laptop as it existed prior to its seizure on October 17, 2006. It should also be noted that the FBI participated in the spoliation on October 20, 2006, when FBI SA Slinkard allowed Hoffman to turn on the Wu laptop and copy the "Private" folder to a USB device. *See* Computer Forensics: Disk Imaging Overview, attached hereto as Exhibit A ("Don't turn the computer on or off, or examine logs, until the disk has been imaged.").

The government's factual misstatements appear to have been advanced as support for two separate, but interconnected contentions. First, that the hash values for the FTK EnCase images of the Wu laptop and the Acronis backup copy "matched" the hash values contained in the "original sources" – *i.e.*, the electronic data in the Wu laptop and the Acronis backup copy as it existed on October 17, 2006. Second, because the hash values match, it is appropriate to simply compare the logical content contained in the FTK EnCase image of the Acronis backup copy with the logical content in the FTK EnCase image of the Wu Laptop in order to authenticate the electronic data (*i.e.* documents) contained in the FTK EnCase Wu laptop image as having come from the Wu laptop despite its spoliation by Hoffman.

The Government's Brief fails to cite to the record or the hearing transcript of the November 16 motions hearing. The reason for this lack of citation is simple – neither the document record nor the hearing transcript of testimony supports the government's contentions. The government's only attempt to introduce the hash value concept occurred at the very end of Computer Forensics Examiner Johns' redirect examination:

> Q. [AUSA Nyhus] There has been some question or some talk about what an MD5 hash value is. Did you compare the hash values of the images before and after?
>
> A.[Johns] I did.
>
> Q. Were all before hash values compared to and against each other?
>
> A. The imaged files in the case notes, yes. I compared both before and after.
>
> Q. So the hash values, did they match?

A.	Yes, they did.

RT 170.

As is evidenced by the transcript text quoted above, Johns did not offer any testimony comparing the hash values of the FBI's FTK EnCase images and "the original values made of the Wu laptop and the Acronis copy" as the government contends in its brief. (Government's Brief at p. 4). Moreover, there was no testimony during the course of the motions hearing that hash values for the original Wu laptop and the Acronis copy on the USB device had been generated prior to the FBI's FTK imaging activity. Indeed, any such testimony would have been suspect in that the Acronis backup software does not support hash valuation.[2] Finally, during recross-examination, Johns admitted that the hash values he had examined related only to the images themselves, and that his examination had been restricted to review of FBI SA Brillhart's paperwork:

Q. [AFPD Schatz]	In terms of the hash values that you compared, **is it not the case that those are the hash values simply of the imaged files themselves**, not of the content?
A. [Johns]	**Yes**.
Q.	And those - - that analysis you did with respect to the hash values is simply **of the imaged files themselves**, that was done by looking at the paperwork; is that correct?
A.	**Correct**.
Q.	You didn't look at the image?

[2] Although the FTK EnCase image of the Acronis backup copy has a hash value, the USB resident Acronis backup copy did not have a hash value function. Acronis does not generate a hash value for the backup copy itself or for any of the files copied. Consequently, there is no way to tell to what extent the electronic data on the Acronis backup copy was altered, modified, deleted or added to between the time the backup copy was made and the time that the backup copy was imaged by the FBI.

A. I did not.

RT 171 (emphasis added).[3]

No hash values were generated at the time the Wu laptop was taken from Wu by Hoffman and delivered into the custody of Mark Hansen. That the hash values of the subsequently generated FTK EnCase images of the Wu laptop, following the spoliation of its electronic data by Hoffman and others, match is simply irrelevant. There is simply no baseline for comparison that will allow any one with forensic computing expertise to conclude that the contents of the FTK EnCase image of the Wu laptop are identical to the contents of the Wu laptop prior to its seizure.[4]

Furthermore, merely comparing the logical content in the FTK EnCase Acronis backup copy image with the logical content in the FTK EnCase Wu laptop image also fails as an authentication method.[5] Insofar as Acronis backup software does not support a hash value function, there is no way

[3] When the FTK image was created the FTK software automatically generated an Md5 hash value for the image itself, which SA Brillhart presumably recorded in the NWRFCL case file. It is unclear whether Johns, in conducting his administrative review, actually compared that Md5 hash value with the image itself or simply with notations in the paperwork pertaining to the same image when subsequently reviewed or replicated.

[4] The FTK EnCase image of the Acronis backup copy cannot serve as a baseline for comparison because, although the image itself has a hash value, the Acronis backup copy software did not support a hash value function and therefore there is no known hash value for the Acronis backup copy that can be compared with either the hash value of the Acronis backup copy FTK EnCase image or the Wu laptop FTK EnCase image.

[5] Logical content comparison can be pursued through analysis of the native file format of the electronic data that is the target of analysis and/or by simply printing documents from various sources for visual inspection. But logical content comparison cannot detect, let alone protect against, intentional spoliation of electronic data by alteration, amendment, or deletion. Consequently, while printed hard copies of electronic documents may appear identical, a visual comparison process standing alone cannot serve to confirm the authorship of the documents, the time of their creation, the extent of their subsequent amendment or modification, or the original source of the documents.

any one can conclude with a reasonable degree of certainty that the electronic data in the Acronis backup copy was not modified, changed and/or deleted prior to the imaging of the Wu laptop hard drive.[6]

Conclusion

The government declined to present expert testimony concerning the procedures followed in generating the FTK images. The government failed to call as a witness the agent who generated the FTK images to testify (*i.e.* FBI SA Brillhart). The government did not produce for review by the Court and counsel the Northwest Regional Computer Forensics Laboratory case file pertaining to the FTK images. The government has ignored the findings of Computer Forensics Expert Michael Bean that potentially material e-mail folders appear to have been deleted from the Wu laptop during the time it was in Hoffman's possession (*see* Supplemental Declaration Of Computer Forensics Expert Michael A. Bean In Support Of Motion To Exclude Images Of The Wu Laptop Hard-Drive [Docket No. 82], at pp. 4-5), and that "over 1000 files or folders . . . were accessed, manipulated, or created after the date of creation associated with Hansen's Acronis backup file" (*see* Declaration of Computer Forensics Expert Michael A. Bean In Support Of Motion To Exclude Images Of The Wu Laptop Hard-Drive [Docket No. 36], at pp. 6-7).

///

///

///

[6] The running of the defrag utility on the Wu laptop further spoliated the electronic data by making it impossible to determine what and/or how much electronic data had been deleted prior to the creation of the FTK EnCase Wu laptop image.

The argument set forth in the Government's Brief is factually misleading and, for the most part, pure *ipse dixit*. As such, its value to the resolution of the important legal issues raised by Mr. Khoo with respect to the authentication of the Wu laptop and Acronis backup copies should be recognized as being nothing more than an *ignis fatuus* – proving nothing and leading nowhere.

Respectfully submitted this January 24, 2011.

/s/ Christopher J. Schatz
Christopher J. Schatz
Attorney for Defendant Hock Chee Khoo